Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1.-5. (Cancelled).

6. (Original) A computer which comprises a system section and an application software section, and which takes in copyright claimed, encrypted data via a digital interface for processing therein, wherein

said system section includes a plurality of tamper verification functions, and a tamper code associated with a designated type of tamper verification function and type information indicating said type are embedded into said application software in said application software section, and wherein said system section reads said tamper code and its associated type information from said application software section and, using the tamper verification function corresponding to said type, verifies whether or not said application software has been tampered with, and if it is found that said application software has been tampered with, said system section reports the result of said verification.

7.-8. (Cancelled).

9. (Currently Amended) A medium holding thereon a program and/or data for enabling a computer to implement all or part of the functions of all or part of the means of the invention described in any one of the claims 6[[-7]], 17-20, or 21, wherein said medium is computer processable.

10. (Currently Amended) A collection of information stored on a computer or a computer readable medium, wherein said collection of information is a program and/or data for enabling a computer to implement all or part of the functions of all or part of the means of the invention described in any one of the claims 6[[-7]], 17-20, or 21.

11. (Previously Presented) In a computer having an operating system and an application program, in which the application program performs a task of providing data to a user, a method of protecting copyrighted received data, comprising the steps of:

(a) receiving by the operating system copyrighted data;

(b) authenticating by the operating system the application program;

(c) encrypting by the operating system the copyrighted data received in step (a);

(d) providing a decryption key from the operating system to the application program, if the application program is authenticated in step (b);

(e) transmitting the encrypted data of step (c) from the operating system to the application program; and

(f) decrypting the encrypted data in the application program using the key provided in step (d); and

step (b) further includes determining a license classification of the application program, in which the classification is one of (i) display-only permitted and (ii) recording permitted.

12. (Previously Presented) The method of claim 11 in which step (c) includes decrypting the data received in step (a) using another key before encrypting the data in step (c).

13. (Previously Presented) The method of claim 11 in which step (b) includes

i) generating a digital signature in the application program;

ii) sending the digital signature from the application program to the operating system and storing the signature in the operating system; and

iii) authenticating the application program using the signature stored in step (ii).

14. (Cancelled).

15. (Previously Presented) The method of claim 11 in which step (a) includes receiving at least one of copyrighted audio data and copyrighted video data.

16. (Previously Presented) The method of claim 11 in which the operating system controls allocation and usage of resources of the computer.

17. (Previously Presented) In a computer having an operating system and an application program, and receiving copyrighted data via a digital interface for processing,

a method of protecting the received data comprising the steps of:

(a) providing a plurality of tamper verification functions to the operating system;

(b) providing a tamper code, associated with a designated type of tamper verification function, to the application program;

(c) receiving, by the operating system, copyrighted data;

(d) reading, by the operating system, the tamper code and its associated type information from the application program;

(e) using, by the operating system, the tamper code and associated type information with a corresponding tamper verification function to verify whether or not the application program has been tampered with, and if it is found that the application program has been tampered with, the operating system reports the results of the verification,

(f) determining a license classification of the application program, in which the classification is one of: (i) display-only permitted, and (ii) recording permitted;

(g) encrypting, by the operating system, the received copyrighted data;

(h) if the operating system verifies that the application program (i) has not been tampered with, and (ii) has a proper license classification, then providing, by the operating system, the encrypted data and a decryption key to the application program; and

(i) decrypting the encrypted data in the application program using the decryption key from the operating system.

18. (Previously Presented) A computer having a system section and an application software section, and which takes in copyright claimed, encrypted data via a digital interface for processing therein, wherein

said system section judges that said application software section is legitimate application software for the protection of copyright,

if said application software is a legitimate one, said system section passes a key for said encrypted data to said application software section,

said judgment in said system section is made by using a CRL (Certification Revocation List) listing illegitimate or legitimate application software, and listing at least tamper type information,

said system section includes a plurality of tamper verification functions, and a tamper code associated with a designated type of tamper verification function and type information indicating said type are embedded into said application software in said application software section, and

said system section reads said tamper code and its associated type information from said application software section and, using the tamper verification function corresponding to said type, verifies whether or not said application software has been tampered with, and if it is found that said application software has been tampered with, said system section reports the result of said verification.

19. (Previously Presented) In a computer having a system section and an application software section, and which takes in copyright claimed, encrypted data via a digital interface for processing therein, a method comprising the steps of:

judging, by said system section, that said application software section is a legitimate application software for the protection of copyright,

if said application software is a legitimate one, passing, by said system section, a key for said encrypted data to said application software section,

wherein said judgment in said system section is made by using a CRL (Certification Revocation List) listing illegitimate or legitimate application software, and listing at least tamper type information,

said system section includes a plurality of tamper verification functions, and a tamper code associated with a designated type of tamper verification function and type information indicating said type are embedded into said application software in said application software section, and

reading, by said system section, said tamper code and its associated type information from said application software section, and

using the tamper verification function corresponding to said type, verifying whether or not said application software has been tampered with, and if it is found that said application software has been tampered with, reporting, by said system section, the result of said verification.

20. (Previously Presented) A computer having a system section and an application software section, and which takes in copyright claimed, encrypted data via a digital interface for processing therein, wherein

said system section judges that said application software section is legitimate application software for the protection of copyright,

if said application software is a legitimate one, said system section passes a key for said encrypted data to said application software section,

said judgment in said system section is made by using a CRL (Certification Revocation List) listing illegitimate or legitimate application software, and listing at least tamper type information,

said system section includes a plurality of tamper verification functions, and a tamper code associated with a designated type of tamper verification function and type information indicating said type are embedded into said application software in said application software section, and

said system section reads said tamper code and its associated type information from said application software section and, using the tamper verification function corresponding to said type, verifies whether or not said application software has been tampered with, and if it is found that said application software has been tampered with, said system section reports the result of said verification,

said system section is configured to send said data to said application section by embedding into said data information concerning application software residing in said application software section,

wherein the information concerning said application software is information indicating the name of said application software, or the version number of said application software, or a tamper code, or the type of a tamper resistance verification function, or information concerning a user.

21. (Previously Presented) In a computer having a system section and an application software section, and which takes in copyright claimed, encrypted data via a digital interface for processing therein, a method comprising the steps of:

judging, by said system section, that said application software section is a legitimate application software for the protection of copyright,

if said application software is a legitimate one, passing, by said system section, a key for said encrypted data to said application software section,

wherein said judgment in said system section is made by using a CRL (Certification Revocation List) listing illegitimate or legitimate application software, and listing at least tamper type information,

said system section includes a plurality of tamper verification functions, and a tamper code associated with a designated type of tamper verification function and

type information indicating said type are embedded into said application software in said application software section, and

reading, by said system section, said tamper code and its associated type information from said application software section, and

using the tamper verification function corresponding to said type, verifying whether or not said application software has been tampered with, and if it is found that said application software has been tampered with, reporting, by said system section, the result of said verification,

wherein said system section sends said data to said application section by embedding into said data information concerning application software residing in said application software section, and

the information concerning said application software is information indicating the name of said application software, or the version number of said application software, or a tamper code, or the type of a tamper resistance verification function, or information concerning a user.